FINITE GROUPS WITH ALL MAXIMAL SUBGROUPS OF PRIME OR PRIME SQUARE INDEX

JOSEPH KOHLER

1. Introduction. In this paper finite groups with the property M, that every maximal subgroup has prime or prime square index, are investigated. A short but ingenious argument was given by P. Hall which showed that such groups are solvable.

B. Huppert showed that a finite group with the property M^1 , that every maximal subgroup has prime index, is supersolvable, i.e. the chief factors are of prime order. We prove here, as a corollary of a more precise result, that if G has property M and is of odd order, then the chief factors of G are of prime or prime square order. The even-order case is different. For every odd prime p and positive integer m we shall construct a group of order $2^a p^b$ with property M which has a chief factor of order larger than m.

These results can be stated in another form by using a theorem due to Huppert (7, Satz 1). If G is a finite group with property M^1 , then all subgroups of G have property M^1 and if G has property M with |G| odd, then all subgroups of G have property M.

The author wishes to express his sincere appreciation to his former advisor Professor Marshall Hall, Jr., for his interest, guidance, and patience. Special thanks are due to Dr. C. R. B. Wright and Dr. S. Golomb for their encouragement during the preparation of this paper.

2. Notations and definitions. The following is a list of notations which will be used: |G| = the order of G; H < G means H is a subgroup of G; Z(G) = the centre of G; $\Delta(G) =$ the intersection of the non-normal maximal subgroups of G; $\phi(G) =$ the Frattini subgroup of G; $J_p =$ the field with p elements; GL(n, p) = the group of non-singular $n \times n$ matrices over J_p ; $\langle A, B \rangle =$ the group generated by the subsets A and B of G; (A, B) = commutator subgroup of A and B; $G^n = \langle X^n | X \in G \rangle$.

Definition. Let p be a prime which divides |G|, where G is solvable. If among the chief factors of G which have order a power of p the exponent s is the largest one that occurs, then s is the p-rank of G. This will be denoted by $r_p(G)$.

3. The main theorems. Let G be a group with property M. By (4,

Received February 4, 1963. This work was sponsored in part by the Jet Propulsion Laboratory of Pasadena, California. The paper is based on the author's PH.D. dissertation submitted to the California Institute of Technology in 1962.

Theorem 10.5.7), G is solvable. However, the proof yields more information. This we state as the following theorem.

THEOREM 3.1 (P. Hall). Let G be a group with property M. Then there exists a normal series G > K > 1 with |K| prime to 6, $|G/K| = 2^{a}3^{b}$, and K has an ordered Sylow tower.

Proof. See the proof of (4, Theorem 10.5.7).

If 2 does not divide |G|, then G has an ordered Sylow tower. The same is true if 3 does not divide |G|.

LEMMA 3.1. A subgroup K of GL(2, p) which has odd order prime to p is abelian.

Proof. For p = 3 the lemma is trivial. Thus we may assume that p > 3. The group GL(2, p) has a normal subgroup G of index 2 consisting of those matrices whose determinant is a square. We observe that G > K and G > Z, the centre of GL(2, p) consisting of all scalar multiples of the identity. A list of subgroups of G/Z can be found in (2, pp. 447–450). The subgroups of odd order prime to p are cyclic, and this order is a divisor of p + 1 or p - 1. Thus KZ/Z is cyclic and therefore KZ is abelian. Hence K is abelian.

LEMMA 3.2. Let G be a finite abelian group and let ρ be an irreducible representation of G over the field F. Then $\rho(G)$ is cyclic.

Proof. Let A be an F-G module, which yields the representation ρ . Since A is irreducible, it follows from Schur's lemma that the ring of operator endomorphisms of A forms a division ring D. D is isomorphic to the ring of square matrices whose elements α satisfy $\rho(x)\alpha = \alpha\rho(x)$ for every x in G (4, Corollary 16.6.1). But the matrices $\rho(x)$ for x in G are among the choices for α and therefore belong to the centre of D. Hence $\rho(G)$ is a finite subgroup of the multiplicative group of a field and therefore cyclic.

LEMMA 3.3. Let G be an irreducible subgroup of GL(2, p) with |G| odd. Then G is cyclic and |G| divides $p^2 - 1$.

Proof. By Lemma 3.1, G is abelian and by Lemma 3.2, G is cyclic.

Let A, ρ , and D be the same as in the preceding lemma for the group $G = \langle g \rangle$ and the field $F = J_p$. If $a \neq 0$ with a in A, then A is spanned by the vectors $a_i = \rho(g^i), i = 0, 1, \ldots$, since ρ is irreducible. Since A is a cyclic $\rho(g)$ module, any linear transformation on A which commutes with $\rho(g)$ is in the algebra spanned by $\rho(g^i), i = 0, 1, \ldots$. But D is just the set of linear transformations on A which commute with $\rho(g)$. Thus D is the field spanned by the $\rho(g^i),$ $i = 0, 1, \ldots$, from which it follows that (D:F) equals the dimension n of Aover J_p . Every non-zero element X of the field D satisfies $X^{p^n-1} = 1$.

For the lemma, n = 2 and $g = \rho(g)$, giving $g^{p^2-1} = 1$.

436

LEMMA 3.4. Let G be a cyclic group whose order is a divisor of $p^2 - 1$. Then every irreducible representation of G over J_p has degree one or two.

Proof. The second paragraph of the above proof applies. Note that D can be regarded as F with $\rho(g)$ adjoined. Thus $X^{p^2-1} = 1$ for all X in D. Hence the degree of D over F is 1 or 2 so that A has dimension 1 or 2 over J_p , proving the lemma.

LEMMA 3.5. Let G be an abelian group of exponent dividing $p^2 - 1$. Then every irreducible representation of G over J_p has degree one or two.

Proof. Let ρ be an irreducible representation of G over J_p . By Lemma 3.2, $\rho(G)$ is cyclic and by hypothesis $\rho(G)$ has order dividing $p^2 - 1$. By Lemma 3.4, $\rho(G)$ has degree one or two.

The author is grateful to the referee for pointing out the following theorem.

THEOREM 3.2. If G is a finite solvable group and p any prime, let $S_p(G)$ denote the largest integer such that G has a maximal subgroup of index p^s . Then

(1) $S_p(G) = 1$ implies $r_p(G) = 1$;

(2) $S_p(G) = 2$ and |G| odd imply $r_p(G) = 2$.

Proof. We prove (2) by induction on |G|. Let $K = G^{p^2-1}G'$, so that G/K is the largest abelian quotient group of G having exponent $p^2 - 1$. We may assume that $K \neq 1$. Let M be a minimal normal subgroup of G contained in K. Then $S_p(G/M) \leq 2$ and |G:M| is odd, so that $r_p(G/M) \leq 2$ by induction. This gives $r_p(G) \leq 2$ unless $|M| = p^s$ with s > 2.

Assume s > 2. Let *C* be the centralizer of *M* in *G*. If C > K, then by Lemma 3.5 we have $s \leq 2$, so that $D = K \cap C < K$; $D \neq K$ There is a chief factor E/D of *G* with E < K and $E/D \cong CE/C$, which is a minimal normal subgroup of G/C. Now G/C is isomorphic to an irreducible subgroup of GL(s, p) and therefore cannot have a normal *p*-subgroup so that CE/C and hence E/D has order prime to *p*. Therefore, if *Q* is a Sylow *p*-complement of *K*, then E < DQ.

Consider the representation ρ of G on one of its chief p-factors in K/M. Since $r_p(G/M) \leq 2$, it follows from Lemma 3.3 that $G/\ker p$ is cyclic and has order dividing $p^2 - 1$. Thus ker $\rho > K$ so that K centralizes all chief pfactors of K/M. Hence K/M has a normal p-complement MQ/M. Here MQ/M is a characteristic subgroup of K/M so that MQ is a proper normal subgroup of G.

Let N be the normalizer of Q in G. Then MN = G, since Q^x is conjugate to Q in MQ for all x in G. Since M is abelian and normal in G, $M \cap N$ is a proper normal subgroup of MN = G. If N > M, then (M, Q) = 1 so that Q < C. But Q < C implies DQ < C and thus $E < C, E \neq C$, a conflict. Hence $N \gg M$. Owing to the minimality of M, the only alternative is that $M \cap N = 1$. Thus N is a maximal subgroup of G with $|G:N| = p^s$, which contradicts $S_p(G) = 2$. This proves (2). The proof of (1) is similar but simpler.

JOSEPH KOHLER

THEOREM 3.3. Let G be a group of odd order which has property M. Then $r_p(G) \leq 2$ for all primes p which divide |G|.

Proof. By Theorem 3.1, G is solvable. The theorem follows at once from Theorem 3.2.

THEOREM 3.4. Let G be a group of odd order which has property M. Then all subgroups of G also have property M.

Proof. This is an immediate consequence of Theorem 3.3 together with **(7**, Satz 1).

4. Construction of examples. In this section examples of groups of order $2^a p^b$, p an odd prime, will be constructed which have property M but contain subgroups which do not have this property. In fact given any positive integer m such a group will be constructed which has a subgroup containing a maximal subgroup of index at least m.

LEMMA 4.1. Let G be a group and let G_{t+1} be the (t + 1)st term in the descending central series of G. Then

$$(a_1,\ldots,x_y,\ldots,a_t) \equiv (a_1,\ldots,x,\ldots,a_t)(a_1,\ldots,y,\ldots,a_t) \pmod{G_{t+1}}.$$

Proof. (6, Theorem 2.84).

Let p be an odd prime. Let D be the subgroup of GL(2, p) which is generated by

$$x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
 and $y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

D is absolutely irreducible and |D| = 8. Let $K = A_1 * \ldots * A_t$ be the free product of the groups A_1, \ldots, A_t , where each A_i is elementary abelian and of order p^2 . Suppose that $A_i = \langle a_i, b_i \rangle$. Define

$$a_i{}^{x_i} = a_i, \qquad a_i{}^{y_i} = b_i{}^{-1}, \\ b_i{}^{x_i} = b_i{}^{-1}, \qquad b_i{}^{y_i} = a_i,$$

for i = 1, ..., t. Then $H_i = \langle x_i, y_i \rangle$ is a group of automorphisms of A_i which is isomorphic to D. We extend H_i to a group of automorphisms of K by assuming that each element of H_i induces the identity on A_j for $j \neq i$. The group $\langle H_1, ..., H_i \rangle = H$ is a group of automorphisms of K and

$$H = H_1 \times \ldots \times H_t.$$

Let K_{t+1} be the (t + 1)st term of the descending central series of K. Since K_{t+1} is characteristic in K, it follows that H induces automorphisms on K/K_{t+1} . Also the group $L = K/K_{t+1}$ is a finite p-group since it is nilpotent and generated by finitely many elements of order p.

A commutator of the form $(\alpha_1, \ldots, \alpha_t)$, where $\alpha_i = a_i$ or $\alpha_i = b_i$ is said to be of type A. Let G denote the semi-direct product of L by H. Let W denote the subgroup of G which is generated by the commutators of type A.

https://doi.org/10.4153/CJM-1964-046-6 Published online by Cambridge University Press

438

LEMMA 4.2. W is a normal, elementary abelian p-subgroup of G which is in the centre of L.

Proof. By (4, Corollary 10.2.1), W is contained in the centre of L, in particular W is abelian. Also a commutator of type A has order $p \pmod{K_{t+1}}$ or else is the identity (mod K_{t+1}). This follows from

$$1 \equiv (\alpha_1^p, \alpha_2, \ldots, \alpha_t) \pmod{K_{t+1}}.$$

since $\alpha_i^p = 1$ in K. But

$$(\alpha_1^p, \alpha_2, \ldots, \alpha_t) \equiv (\alpha_1, \alpha_2, \ldots, \alpha_t)^p \pmod{K_{t+1}}$$

by Lemma 4.1. Each element in G has a unique representation in the form kh where $k \in L$ and $h \in H$. Then for $(\alpha_1, \ldots, \alpha_t) K_{t+1}$ in W we have

$$[(\alpha_1,\ldots,\alpha_l)K_{l+1}]^{kh} = (\alpha_1,\ldots,\alpha_l)^{kh}K_{l+1}.$$

Now *h* can be written in the form $h = h_1 h_2 \dots h_i$, where $h_i \in H_i$ for $i = 1, \dots, t$. Since h_i and h_j commute for $i \neq j$ and h_i centralizes A_j for $j \neq i$, we conclude that

$$(\alpha_1,\ldots,\alpha_t)^h K_{t+1} = (\alpha_1^{h_1},\ldots,\alpha_t^{h_t}) K_{t+1}.$$

But $\alpha_i^{h_i}$ is either a_i^{ϵ} or b_i^{δ} , where $\epsilon = \pm 1$ and $\delta = \pm 1$. So by Lemma 4.1, a commutator of type $A \pmod{K_{t+1}}$ under an element of G is again a commutator of type A or else the inverse of such a commutator. Hence W is a proper normal subgroup of G.

LEMMA 4.3. The commutators of type A (mod K_{t+1}) are a basis for W.

Proof. We must prove the independence of the commutators of type A (mod K_{t+1}). Suppose that

(1)
$$\Pi(\alpha_1,\ldots,\alpha_t)^{\theta(\alpha_1,\ldots,\alpha_t)} \equiv 1 \pmod{K_{t+1}},$$

where the product extends over the commutators of type A and at least one $\theta(\alpha_1, \ldots, \alpha_t)$ is not congruent to zero (mod p). Without loss of generality we may assume that $\theta(\alpha_1, \ldots, \alpha_t) \not\equiv 0 \pmod{p}$. Then

$$(a_1, \ldots, a_t)^{\theta(a_1, \ldots, a_t)} \equiv 1 \pmod{\tilde{K}_{t+1}},$$

where $\bar{K} = \langle a_1 \rangle * \ldots * \langle a_i \rangle$. Here we are using the fact that there is a homomorphism of K onto \bar{K} which maps each b_i into 1 and each a_i into itself. Raising both sides of this relation to a suitable power yields

(2)
$$(a_1,\ldots,a_t) \equiv 1 \pmod{\bar{K}_{t+1}}.$$

By (4, Theorem 12.1.1), any group $T = \langle c_1, \ldots, c_t \rangle$ with $c_i^p = 1$ for $i = 1, \ldots, t$ is a homomorphic image of \bar{K} under the correspondence $a_i \to c_i$. If T_{t+1} is the identity, then the kernel of this homomorphism contains \bar{K}_{t+1} . Hence the mapping $a_i \bar{K}_{t+1} \to c_i$ is a homomorphism from \bar{K}/\bar{K}_{t+1} onto T. We shall construct a group $T = \langle c_1, \ldots, c_i \rangle$ with $c_i^p = 1$, $T_{t+1} = 1$, and $(c_1, \ldots, c_i) \neq 1$. This will contradict relation (2) and prove that (1) cannot hold. The elements of T are square matrices of size (t + 1) with entries from J_p . Let I be the identity matrix and E_{ij} be the matrix with a 1 in position (i, j) and zeros elsewhere. Let $c_i = I + E_{i+1,i}$ for $i = 1, \ldots, t$. The inverse of c_i is $I - E_{i+1,i}$, and $(c_1, \ldots, c_t) = I + \epsilon E_{t+1,1}$, where $\epsilon = \pm 1$ depending upon whether t is even or odd. In either case $(c_1, \ldots, c_t) \neq 1$.

As a consequence of Lemma 4.2, W can be regarded as a vector space on which G operates. By Lemma 4.3, a basis for this vector space is given by the commutators of type A. Using this basis it is easy to see that the representation which G induces on W is the Kronecker product of t groups isomorphic with D and is therefore absolutely irreducible. Hence W is a chief factor of G.

THEOREM 4.1. G has property M, but its subgroup HW contains H as a maximal subgroup and $|HW:H| = p^{2^t}$.

Proof. If M is a maximal subgroup of G, then M must contain the commutator subgroup L' of $L = K/K_{t+1}$. For L' is a proper normal subgroup of G, and if $L' \leq M$, then L'M = G, $L'(M \cap L) = L$ and therefore $M \cap L = L$ by (4, Corollary 10.3.3), which is a contradiction. The maximal indices of G are the same as those of G/L'. But the chief factors of G/L' have orders 2 or p^2 so that $S_p(G) = 2$, $S_2(G) = 1$. Thus G has property M.

Consider the subgroup HW of G. W is operated on absolutely irreducibly by H and therefore H is a maximal subgroup of HW. Note that $|HW:H| = |W| = p^{2^t}$.

5. Two theorems on groups with property M. By a theorem of Gaschutz (3, Satz 16) $\Delta(G)$ is a nilpotent subgroup of G. Groups with property M can be characterized by the factor group $G/\Delta(G)$.

LEMMA. If G is a subdirect product of primitive solvable groups on a prime or prime square number of letters, then $r_p(G) \leq 2$ for every prime p which divides |G|.

Proof. It is sufficient to prove the lemma for primitive solvable groups on a prime or prime square number of letters. A primitive solvable group T contains a unique minimal normal subgroup B and T/B is isomorphic to a group of automorphisms of B. Also |B| equals the degree of T. If |B| = q, a prime, then T/B is cyclic and $r_p(T) = 1$ for all primes p which divide |T|. If $|B| = q^2$, then examination of the solvable subgroups of GL(2, q) shows that $r_p(T/B) \leq 2$ for all primes p which divide |T/B|.

THEOREM 5.1. A finite group G has property M if and only if $G/\Delta(G)$ is isomorphic to a subdirect product of primitive solvable groups on a prime or prime square number of letters.

440

Proof. Assume that $G/\Delta(G)$ has the above property. The lemma and (3, Satz 16) imply that $r_p(G) \leq 2$ for all primes p which divide |G|. By (7, Satz 1), G has property M.

Assume that G has property M. Decompose the maximal subgroups of G into conjugate classes and represent G by conjugation on these classes. This gives a permutation representation π , where the sets of transitivity are just the sets of conjugate maximal subgroups. Consider the restriction of π to one of these sets. If M is an element of this set, the restricted representation π^* is equivalent to that arising from the cosets of N(M), the normalizer of M in in G; cf. (2, p. 242).

The group N(M) is equal to G or M. If G, then π^* is the identity; and if M, then π^* is primitive of degree |G:M|, which is a prime or the square of a prime. Hence G modulo the kernel of π is a subdirect product of primitive solvable groups on a prime or prime square number of letters.

We determine the kernel of π . An element x of G will be in this kernel if and only if it normalizes every maximal subgroup of G. A non-normal maximal subgroup of G is its own normalizer so that the kernel of π is $\Delta(G)$.

THEOREM 5.2. Let G be a group whose order is not divisible by 6. If every maximal subgroup of G has property M, then G is solvable.

Proof. Use induction on |G|. The hypothesis is satisfied by all factor groups of *G*. Let *M* be any maximal subgroup of *G*. By Theorem 3.1, *M* has an ordered Sylow tower. Let *p* be the smallest prime which divides |G| and let *P* be a Sylow *p*-subgroup of *G*. Let *N* be the normalizer of *P* in *G*. By induction every proper subgroup of *G* has an ordered Sylow tower.

Assume G is p-normal. If N = G, then P is a solvable normal subgroup of G and the proof is completed by induction. If N is a proper subgroup of G, then it has an ordered Sylow tower, so that N contains a normal p-complement. By Theorem (4, 14.4.6), G contains a normal subgroup with a p-factor group. This normal subgroup has an ordered Sylow tower and therefore G is an extension of a solvable group by a p-group. Thus G is solvable.

Assume that G is not p-normal. By (4, Lemma 19.3.2), G satisfies the hypothesis of a theorem of Burnside (4, Theorem 4.2.5). Hence G contains a p-subgroup $H = h_1h_2 \ldots h_r$, where each h_i is a proper normal subgroup of H. The groups h_1, h_2, \ldots, h_r form a complete set of conjugates in N(H), the normalizer of H in G, and r > 1 is prime to p. If H is not normal in G, then N(H) is a proper subgroup of G and has an ordered Sylow tower. Hence N(H) contains a normal p-complement K. Thus (K, H) = 1 so that $N(H) = K \times H$. Thus N(H)/C(H) is a p-group, where C(H) denotes the centralizer of H in G. But h_1, \ldots, h_r form a complete set of conjugates in N(H) so that N(H)/C(H) has order divisible by r. This contradiction proves that it is a proper normal subgroup of G.

This theorem is not true if 6 divides |G|. The linear fractional groups LF(2, p)

are simple for p > 3. From the discussion given in (2, Chapter 20), it follows that the maximal subgroups of LF(2, p) all have property M, if p is not congruent to $\pm 1 \pmod{5}$.

References

- 1. A. A. Albert, Fundamental concepts of higher algebra (Chicago, 1956).
- 2. W. Burnside, Theory of groups of finite order, 2nd ed. (New York, 1955).
- 3. W. Gaschutz, Über die ϕ -Untergruppe endlicher Gruppen, Math. Z., 58 (1953), 160-170.
- 4. M. Hall, The theory of groups (New York, 1959).
- P. Hall and G. Higman, On the p-length of p-soluble groups and reduction theorems for Burnside's problem, Proc. Lond. Math. Soc., 6 (1956), 1-42.
- P. Hall, A contribution to the theory of groups of prime power order, Proc. Lond. Math. Soc. (2), 36 (1933), 29–95.
- 7. B. Huppert, Normalteiler und maximale Untergruppen endlicher Gruppen, Math. Z., 60 (1954), 409-434.

California Institute of Technology Pasıdena, California